REMARKS

Applicant respectfully submits that all the claims presently on file are in condition for allowance, which action is earnestly solicited.

THE CLAIMS

Claim Rejection under 35 USC 102

Claims 1-9, 19-31, and 33-39 were rejected under 35 U.S.C. 102(a) as being anticipated by De La Huerga, US patent 5,960,085. Applicant respectfully submits that De La Huerga does not disclose all the elements and limitations of the rejected claims, as amended. Consequently, the claims on file are not anticipated under 35 U.S.C. 102, and the allowance of these claims is earnestly solicited. In support of this position, Applicant submits the following arguments:

A. Legal Standard for Lack of Novelty (Anticipation)

The standard for lack of novelty, that is, for "anticipation," is one of strict identity. To anticipate a claim for a patent, a **single prior source must contain** all its essential elements, and the burden of proving such anticipation is on the party making such assertion of anticipation. Anticipation cannot be shown by combining more than one reference to show the elements of the claimed invention. The amount of newness and usefulness need only be minuscule to avoid a finding of lack of novelty.

The following are two court opinions in support of Applicant's position of non anticipation, with emphasis added for clarity purposes:

- "Anticipation under Section 102 can be found only if a reference shows **exactly** what is claimed; where there are **differences** between the reference disclosures and the claim, a rejection must be based on obviousness under Section 103." *Titanium Metals Corp. v. Banner*, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985).

- "**Absence** from a cited reference **of any element** of a claim of a patent negates anticipation of that claim by the reference." *Kloster Speedsteel AB v. Crucible Inc.*, 793 F.2d 1565, 230 USPQ 81 (Fed. Cir. 1986), on rehearing, 231 USPQ 160 (Fed. Cir. 1986).

B. Brief Summary of the Present Invention

Prior to presenting substantive arguments in favor of the allowability of the claims on file, it might be desirable to briefly review the present invention. The present invention generally relates to the use of personal encoded identification media for **providing time-limited access** to people, objects, information, services, and other resources.

A specific feature of the **time-limited tracking system is to provide concurrent time-limited access** to a large number of people, objects, information, services, and other resources that are collectively referred to as "resources". For example, **the time-limited tracking system allows persons to be tracked only during predetermined (or selected) hours, such as regular business hours, but not during undesirable (or unavailable) hours, such as lunch or break times**. This will allow privacy of movement during the employee's personal time.

Alternatively, the time-limited tracking system could be automatically tied to events in a person's or group's calendar, to allow tracking during important meetings or phone calls, so that an assistant might try to locate individuals during these important events.

The foregoing and other objects and features of the present invention are realized by a time-limited tracking system that includes a transmitter module incorporated in an ID badge, card, or label, and a receiver module incorporated in a secure server. The transmitter module contains a microprocessor and a watch crystal that keeps track of time. **The microprocessor encrypts time with a private, non-public key**, and transmits the encrypted time once every ten seconds. The transmission can be any wireless means, including infrared, radio frequency, electric field, magnetic field, ultrasonics, and so forth. The limited tracking system is capable of individually tracking a large number of receivers that are distributed about one or multiple tracking environments or ranges.

The secure server stores the private keys of all the users (or receivers). The user of the badge can give a third party, or multiple parties, referred to herein as finder, access to the user for specified time periods. As an example, if the user wishes to give the finder tracking access for specific time periods, the user instructs the server to deliver a list of encrypted codes with the user's private key for these time periods. This list can be transmitted or otherwise provided to the finder for storage on the finder's own server. When the finder detects a transmission from the user's badge, the finder's server looks up the current value of the user's badge from the list and compares it to the encrypted code it received from the badge. If a match exists, the finder would have identified and located the user.

The present invention sends the encrypted temporal sequence that appears to the observer as a random number, **and which does not contain a public ID, thus preventing an observer from identifying and tracking the location of a badge**.

C. Independent Claim 1 in Light of De La Huerga

As indicated in the title of the present application, in the specification, and in the claims, **a distinctive and important feature is to provide time-limit access to resources.** As an example, and as explained above in the "Brief Summary of the Present Invention," the present invention limits the time that a system may track an individual to business hours but not during lunch breaks. **De La Huerga does not teach time-limited access.** In conclusion, the present invention teaches time-limited access to resources, while the relied upon reference teaches an authentication method without any means to temporally limit access.

Independent claim 1, as now amended, explains how the time-limited access feature is implemented by one embodiment of the present invention. More specifically, claim 1 states that the subset corresponds to a specific time window during which access to the resource is authorized, so that the authenticator is capable of authenticating the identification medium without resorting to the private key, and only during the specific time window corresponding to the subset of the encrypted code elements, by mapping the subset of the encrypted code elements (TBn)Kn, in order to enable time-limited access to the resource during the specific time window.

De La Huerga teaches limiting access to computer networks through cryptographic exchange (reference is made to Col. 4, lines 59-63), much like a password limits computer access. The "time stamps" taught in De La Huerga (Col. 21, lines 48-50) are used to log data on the security card, for example associating a medication dispensation record with the badge wearer (Col. 22, lines 5-9). De La Huerga does not teach how "time stamps" may be used to provide temporal limits on resource access. Rather, De La Huerga teaches how "time stamps" may be used as an audit tool for marking events and data recorded on the badge (Figure 10).

More specifically, **time stamps cannot be analogized to the encrypted code elements** as recited in claim 1, in that:

(1) The private key with which the encrypted code elements are encrypted is unique to the identification medium. On the other hand, the time stamps are not related to the identification medium.

(2) Contrary to the present invention, De La Huerga does not use time stamps to access the resource.

(3) De La Huerga uses time outs to limit access to the resource, while according to the present invention, the encrypted code elements are used to provide time limited access to the resource, that is the encrypted code elements grant access and then terminate the granted access to the resource.

More specifically, De La Huerga teaches a security badge that sends a key ID tag which a receiving station uses to locate a public key identification signal (Col. 15 lines 56-61 and Col. 16 lines 12-14). An interrogation station can use the

key ID to associate a person with a badge, and track the person without knowing their private key. The present invention sends an encrypted temporal sequence, which appears to the observer as a random number, and which does not contain a public ID, thus preventing an observer from identifying and tracking the location of a badge.

The "Background of the Invention" section of the present application clearly distinguishes over conventional systems (such as De La Huerga) that use public keys, and clearly indicates at page 13 lines 4-8 (of the present application), "that the signal or code transmitted by the badge Bn, includes the badge's time encrypted by the private key Xn, but does not include a public ID as was taught by conventional tracking systems. As a result, the encrypted code transmitted by the badge Bn can only be decrypted by a private, non-public key which is available only to the server 40 and to the badge Bn."

To conclude, independent claim 1 is allowable for not being anticipated by De La Huerga, and the allowance of claim 1 and the claims dependent thereon is respectfully requested.

D. Independent Claims 43 and 44 in Light of De La Huerga

New independent claims 43 and 44 are not anticipated by De La Huerga for containing generally similar elements and limitations as in claim 1. As a result, claims 43 and 44 are allowable, and such allowance is respectfully requested.

Claims Rejection under 35 USC 103

Claims 10-18 were rejected under 35 U.S.C. 103(a) as being unpatentable over De La Huerga. Applicant respectfully submits that this rejection is now moot since the rejected claims depend on the allowable claim 1, and respectfully requests the allowance of these claims.

TELEPHONE INTERVIEW

Applicant and the undersigned attorney of record thank the Examiner for the telephone interview on March 18, 2005, and for the corresponding Interview Summary dated April 7, 2005.

CONCLUSION

All the claims presently on file in the present application are in condition for immediate allowance, and such action is respectfully requested. If it is felt for any reason that direct communication would serve to advance prosecution of this case to finality, the Examiner is invited to call the undersigned at the below-listed telephone number.

Respectfully submitted,

Date: May 7, 2005

Samuel A. Kassatly Law Office
20690 View Oaks Way
San Jose, CA 95120
Tel: (408) 323-5111
Fax: (408) 521-0111

Samuel A. Kassatly
Attorney for Applicant
Reg. No. 32,247a